UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	18 CR 789
	)	
vs.	)	Judge Gary Feinerman
	)	
DENY MITROVICH,	)	
	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

A grand jury charged Deny Mitrovich with knowingly possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). Doc. 1. The court denied Mitrovich's motion to dismiss, which focused on the delay between his arrest and indictment. Doc. 32 (reported at 2019 WL 1773358 (N.D. Ill. Apr. 23, 2019)). Mitrovich now moves to compel the Government to produce discovery concerning the investigative tools used to identify the true IP address of a visitor to a child pornography website—who, by his own admission, was Mitrovich, Doc. 48 at 1, 15; Doc. 56 at 1-2, 4-5, 8-9, 18, 20; Doc. 65 at 2-3, 15-16—despite his use of Tor. Doc. 48. The motion is granted.

Background

Tor—an acronym for "The Onion Router"—is software that allows a computer user to conceal his IP address and location by relaying his internet traffic through the Tor network. Doc. 48 at 2, 12-13; Doc. 56 at 3-6. Tor protects user privacy by passing encrypted data through at least three different servers in the Tor network before sending it to its destination. Doc. 56 at 3 & n.1 (citing *Tor: Overview*, Tor, https://2019.www.torproject.org/about/overview.html.en (last visited Apr. 29, 2020)); *Tor FAQ*, Tor, https://2019.www.torproject.org/docs/faq.html.en (last

visited Apr. 29, 2020); *United States v. Kienast*, 907 F.3d 522, 526 (7th Cir. 2018) ("The Tor software makes user information untraceable by relaying it through a series of interconnected computers."). Tor Browser is a version of Firefox that deploys additional protections to conceal a user's IP address and other identifying information. Doc. 56 at 4-5 & n.3 (citing *Tor FAQ*, *supra*). "Tor has plenty of legitimate uses—think military and law-enforcement officers carrying out investigations, journalists seeking to maintain anonymity, and ordinary citizens researching embarrassing topics. As [one] can imagine, Tor has spawned—and effectively enables—a cache of unsavory sites for black-market trading, child-pornography file-sharing, and other criminal enterprises." *United States v. Taylor*, 935 F.3d 1279, 1282-83 (11th Cir. 2019).

In 2014, the Federal Bureau of Investigation ("FBI") began investigating The Love Zone ("TLZ"), a website that allowed users to advertise and distribute child pornography. Doc. 48 at 1-2; Doc. 65-1 at 1. "In mid-2014, the FBI, MCCU, obtained the ability to identify IP addresses associated with" TLZ, and those addresses "revealed that 'TLZ' was hosted in The Netherlands, with the head administrator residing in Australia." Doc. 65-1 at 1-2; Doc. 48 at 2; *see* Doc. 62 at 8. (MCCU is the former name of the FBI component now called the Child Exploitation Operations Unit. Doc. 62 at 4 n.4.) After the FBI shared that information with Australian authorities, the Queensland Police Service ("QPS") in Australia and the Department of Internal Affairs ("DIA") in New Zealand seized control of TLZ and operated it undercover for several months. Doc. 48 at 2. QPS/DIA arrested a TLZ user, who provided a backup copy of TLZ that included information on user accounts, posts, and messages—including those of a user called "cyberguy"—and QPS/DIA shared that information with the FBI. *Ibid*.

As part of its investigation, QPS/DIA uploaded a hyperlink on TLZ that advertised a child pornography video. Doc. 48 at 3; Doc. 53 at 1-2. According to QPS/DIA, when a TLZ

user clicked on that hyperlink, he was advised that he was attempting to open a file from an external website. Doc. 48 at 3; Doc. 53 at 2. If the user played the file, QPS/DIA could capture his IP address even if it otherwise would have been concealed by Tor. Doc. 48 at 3; Doc. 53 at 2. "Cyberguy" opened the hyperlink and QPS/DIA captured his IP address. Doc. 48 at 3.

Because the IP address indicated that "cyberguy" was located in the United States, Doc. 62 at 8, QPS/DIA provided the lead to the FBI, Doc. 53 at 1. The FBI in turn obtained records from Comcast providing the physical address associated with the IP address. Doc. 48 at 3; Doc. 65-1 at 4. The Government obtained and executed a search warrant for the physical address—Mitrovich's home—and found child pornography videos and photographs stored on hard drives. Doc. 48 at 3-4; Doc. 53 at 1.

As noted, Mitrovich was indicted for possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). Doc. 1. In an effort to obtain information to support a Fourth Amendment challenge to the means used to discover his IP address, Mitrovich served these Criminal Rule 16(a)(1)(E) discovery requests on the Government:

> 4. Any and all discovery relating to the FBI and MCCU[']s "ability to identify IP addresse[s] associated with certain users of TorChat and certain hidden services" as referenced on MITRO_00001. This includes but [is] not limited to the name of the software used, any and all manuals related to the software, logs kept throughout [the] course of [the] investigation, all training materials, including but not limited to training records, certification records, training standards, and training manuals, all policies and procedures regarding use of this software, names and curriculum vitae of any and all individuals who operated [the software], and any and all records utilized by [the] FBI and MCCU during [the] course of this investigation as it relates to this software; and,
>
> 5. Any and all communications between the FBI/MCCU and QPS and DIA throughout Operation Downfall II, as referenced on MITRO_00001-00002, including email communications, letters, and any and all attachments including the reports generated of each user through [the] TLZ sting that were "generated by QPS/DIA and provided to the MCCU for further identification."

Doc. 48 at 4; Doc. 62 at 1-2. The Government responded:

> We will not produce materials in response to #4 because that quoted reference pertains to Operation Downfall Part 1 and is not related to Mitrovich, whose IP address was not obtained in that manner. (His IP address was obtained in Operation Downfall Part 2, when QPS/DIA was operating TLZ in an undercover capacity.)
>
> We will also not produce any materials in response to #5. Even assuming the US government were accountable for the conduct of QPS/DIA (which we dispute), the investigative use of a URL to reveal Mitrovich's true IP address could not have violated the [F]ourth [A]mendment. Among other reasons, Mitrovich had no reasonable expectation of privacy regarding his true IP address when he clicked the URL on TLZ. As a result, discovery pertaining to the relationship between the US and QPS/DIA is not material to the defense, or otherwise discoverable.

Doc. 48 at 5. Mitrovich clarified that Request 4 referred to the software used to direct users from Tor to the external website with the child pornography video file, Doc 48 at 5; Doc. 62 at 1 n.1, but the Government adhered to its objection, Doc. 48 at 5.

Discussion

Mitrovich moves to compel the Government to produce discovery responsive to Requests 4 and 5, arguing that the investigative tools used to reveal his true IP address may have violated the Fourth Amendment, and therefore that *Brady v. Maryland*, 373 U.S. 83 (1963), and Rule 16(a)(1)(E) require disclosure of the requested information to allow him "to properly investigate and research his ability to litigate a motion to suppress." Doc. 48 at 1, 5-17; Doc. 56 at 1-3. Rule 16(a)(1)(E) imposes on Mitrovich the burden to "make at least a *prima facie* showing that the requested items are material to his defense." *United States v. Thompson*, 944 F.2d 1331, 1341 (7th Cir. 1991); *see also United States v. Kohli*, 847 F.3d 483, 493 (7th Cir. 2017). The parties agree that two issues are central to the materiality question: (1) whether the exclusionary rule potentially applies to the conduct of the foreign law enforcement agencies that obtained Mitrovich's IP address; and (2) whether the investigative tools used to identify his IP address

potentially effected a search within the meaning of the Fourth Amendment. If the answer to either question is no, then any Fourth Amendment motion to suppress would be dead in the water, meaning that the discovery Mitrovich seeks would not be material, which in turn means that his motion must be denied. If the answer to both questions is yes, then the discovery is material and Mitrovich's motion must be granted.

A. Foreign Law Enforcement

As to the first disputed issue, the Government contends that the exclusionary rule does not provide a remedy for any action taken by QPS/DIA in the investigation of TLZ and Mitrovich. Doc. 62 at 6-9. "Evidence obtained in a search of an American citizen by foreign authorities operating within their own country is generally admissible in the courts of the United States even if the search does not otherwise comply with … the Fourth Amendment." *United States v. Stokes*, 726 F.3d 880, 890 (7th Cir. 2013). Under the joint venture doctrine, however, "if U.S. agents substantially participate in an extraterritorial search of a U.S citizen and the foreign officials were essentially acting as agents for their American counterparts or the search amounted to a joint operation between American and foreign authorities, the Fourth Amendment generally applies." *Id*. at 890-91.

Citing a March 2015 FBI memorandum concerning the investigation of "cyberguy," Mitrovich argues that the FBI's own description of its cooperation with QPS/DIA shows that the joint venture doctrine applies. Doc. 65 at 2-8; Doc. 65-1. The memorandum reports that the FBI "initiated Operation Downfall II to target [certain] websites," including TLZ, that the FBI "obtained the ability to identify IP addresses associated with … hidden services," including TLZ, and that QPS/DIA acted "[p]ursuant to [that] information." Doc. 65 at 2 (quoting Doc. 65-1 at 1-3). The memorandum adds that QPS/DIA provided the FBI with reports for each TLZ user that

accessed the external child pornography video from an IP address within the United States, that QPS/DIA also provided backup copies of TLZ that contained all user activity on the site, and that the FBI entered the data in a database. Doc. 65-1 at 2-3. Given all this, Mitrovich asserts, the FBI was "working together with foreign law enforcement" in a manner potentially qualifying as a joint venture under *Stokes*. Doc. 65 at 2-5.

The Government counters with the report of an interview that the prosecution team conducted in March 2020—after Mitrovich filed his reply brief in support of the present motion—of FBI Supervisory Special Agent Brooke Donahue. Doc 62 at 4; Doc. 62-1. According to the Government, Special Agent Donahue's description of the TLZ investigation "demonstrate[s] there was no joint venture between the FBI and QPS/DIA," but rather "an arm's length relationship between the FBI and foreign law enforcement authorities that involved deconfliction and lead sharing." Doc. 62 at 7-9. This argument fails at this juncture, where the court must apply the standard governing motions to compel. As the Government acknowledges, "whether the joint venture doctrine is satisfied presents a factually based issue that involves applying a legal label to a complex set of facts." *Id*. at 6 (internal quotation marks omitted) (quoting *United States v. Agosto-Pacheco*, 2019 WL 4566956, at *5 (D.P.R. Sept. 20, 2019)). Because the FBI's contemporaneous March 2015 memorandum makes plausible Mitrovich's submission that there was a joint operation between the FBI and QPS/DIA in connection with the TLZ investigation, he has made "at least a *prima facie* showing" that the joint venture doctrine applies. *Thompson*, 944 F.2d at 1341. It follows that Mitrovich's motion to compel cannot be denied based on the Government's submission that the exclusionary rule does not apply to the investigatory conduct of QPS/DIA in this case.

B. Possible Use of Malware

As to the second disputed issue, Mitrovich contends that the discovery he seeks would allow him to show that his IP address was captured through the installation of malware on his computer, thereby violating the Fourth Amendment. Doc. 56 at 1-2, 7-18; Doc. 65 at 12-17. (For present purposes, the court adopts the Government's broad understanding of Mitrovich's reference to "malware," Doc. 62 at 5 ("QPS/DIA's technique did not involve hacking, using/inserting malware, or using escalated privileges on a user's computer."), which extends beyond the use of a "malicious" bug or virus. *See United States v. Tagg*, 886 F.3d 579, 583 n.2 (6th Cir. 2018) (calling the FBI's technique in that case a "benevolent virus").) The Government does not dispute that the installation of malware on Mitrovich's computer—if it occurred—would have effected a Fourth Amendment search. *See id*. at 584 ("[T]o identify [the website's] users, the FBI had to place a digital bug in the fabric of the website. … [T]his act counts as a Fourth Amendment 'search' of the user's home computer … ."); *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017) (holding that the FBI's sending "computer code to the defendants' respective computers that searched those computers for specific information and sent that information back to law enforcement" was a Fourth Amendment search that "required a warrant"); *United States v. Darby*, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016) (holding that because "[t]he NIT ["Network Investigative Technique"] in this case caused Defendant's computer to download certain code without the authorization or knowledge of Defendant," the Government "invaded the contents of the computer" and its "deployment of the NIT was a Fourth Amendment search"), *aff'd*, 721 F. App'x 304 (4th Cir. 2018).

The Government maintains, however, that QPS/DIA did not deploy malware to discover Mitrovich's true IP address. Doc. 53 at 2 ("QPS/DIA explained that it was able to capture the IP

address by configuring the video file to open an internet connection outside of Tor, thereby allowing QPS/DIA to capture the user's actual IP address, as well as a session identifier that tied the IP address to the activity of a particular TLZ user account."); Doc. 62 at 4 ("[T]he technique … did not involve downloading malware onto [Mitrovich's] computer or otherwise invading the property of his computer."); *id*. at 4-5 (citing Special Agent Donahue's representation during his March 2020 interview that, while he "does not know the 'minute details' of the technique used by QPS/DIA," he "is familiar with what [it] entailed … based on communications he had with Australian/New Zealand law enforcement personnel," and that "there was no information collected from inside the user's computers"). Mitrovich counters that "because of the way the Tor Network and Tor Browser operates, the hyperlink [to the external child pornography video file] must have contained malware that forced [his] computer to send the identifying information to QPS/DIA or forced it to exit from the Tor Browser and onto the open internet." Doc. 56 at 1. According to Mitrovich, the FBI's use of malware to discover IP addresses in other investigations, *see Taylor*, 935 F.3d at 1283 ("As a means of ferreting out [child pornography website] visitors whose identities were masked by Tor, the FBI sought to deploy government-created malware—specifically, a computer code called the Network Investigative Technique ('NIT')—that would transmit user information back to the FBI."), makes it likely that malware was used here as well. Doc. 56 at 7-12. Mitrovich adds that the ability of law enforcement to remove malware from a computer in a manner that prevents a forensic analysis of the computer from revealing its use makes the discovery he seeks the only way to determine whether QPS/DIA in fact used malware. *Id*. at 12-15.

As with his submission that the FBI's cooperation with QPS/DIA potentially calls into play the joint venture doctrine, Mitrovich has made "at least a *prima facie* showing" that

malware was used to obtain his IP address. *Thompson*, 944 F.2d at 1341. It follows that his motion to compel cannot be denied based on the Government's assertion—which rests on second-hand information from QPS/DIA—that malware was not used and therefore that no Fourth Amendment search occurred. *See United States v. Budziak*, 697 F.3d 1105, 1112-13 (9th Cir. 2012) (holding that it was "an abuse of discretion for the district court to deny [the defendant] discovery on the EP2P program," reasoning that "criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary[,] … especially … where … a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software").

Conclusion

Mitrovich's motion to compel is granted. The Government shall produce discovery responsive to Requests 4 and 5 by May 28, 2020, subject to any targeted objections to the production of specific material. By this ruling, the court holds only that Mitrovich has made a *prima facie* showing that the discovery is material to a Fourth Amendment motion to suppress that he might file; this ruling does not speak to the ultimate merits of any such motion.

April 30, 2020

United States District Judge